UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: BRIDGET REARDON, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION and M&T BANK CORPORATION, Defendants.	MDL No. 1:23-mc-03083-ADB-PGL **FIRST AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL** CIVIL ACTION NO. 1:24-cv-11574-ADB

Plaintiff Bridget Reardon ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this first amended class action complaint against defendants Progress Software Corporation ("Progress") and M&T Bank Corporation ("M&T Bank") (collectively, "Defendants"). The following allegations are based upon personal knowledge with respect to Plaintiff's own acts, upon the investigation of her counsel, and upon information and belief as to all other matters:

I. INTRODUCTION

1. This is a putative class action that seeks to remedy Defendants' negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach, which occurred on or about May 27-31, 2023 (the "Data Breach").

2. During the Class Period, Defendants failed to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information, including without limitation, full names, addresses, and M&T Bank checking, savings, and/or money market account

numbers (these types of information, *inter alia,* being hereafter referred to, collectively, as "Private Information," "personally identifiable information," or "PII").[1]

3. Upon information and belief, Plaintiff's and Class Members' Private Information was compromised as a result of a security vulnerability in the MOVEit software, as alleged in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) incorporated and re-alleged herein.

4. Defendants' actions resulting in the Data Breach have impacted approximately 40 million people, through more than 600 organizations, including pension fund management companies, corporations, government agencies, and law and accounting firms.[2]

5. Plaintiff brings this class action complaint to redress injuries related to the Data Breach on behalf of herself and a Nationwide Class of similarly situated persons (defined below).

6. As a direct and proximate result of Defendants' inadequate data security, and breach of its duty to handle PII with reasonable care, Plaintiff's and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals.

7. Plaintiff and the Class, as defined herein, bring claims for negligence, negligence *per se*, breach of contract, breach of third-party beneficiary contract, breach of covenant of good faith and fair dealing, invasion of privacy upon intrusion of seclusion, invasion of privacy upon public disclosure of private facts, unjust enrichment, violation of Massachusetts General Law Ch.

---

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. §200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands.

[2] Raphael Satter & Zeba Siddiqui, *MOVEit hack spawned over 600 breaches but is not done yet—cyber analysts*, REUTERS (Aug. 8, 2023 at 1:18 PM PDT), https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/.

93A, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

8. As a result of the Data Breach, Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: (1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and (3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

II. PARTIES

10. Plaintiff Bridget Reardon is a citizen and resident of the State of New York. Plaintiff is a customer of M&T Bank. On or about August 2023, Plaintiff received a notice from M&T Bank informing Plaintiff that her personally identifying information provided to Progress by M&T Bank was a part of the Data Breach that is the subject of this action ("Notice" attached as Exhibit 1). The Notice advised Plaintiff that there was a "recent global cybersecurity incident involving MOVEit, a file transfer tool owned by Progress Software." The Notice further stated that the "incident resulted in the potential exposure of customer information for any organization using MOVEit." The Notice further informed Plaintiff that M&T Bank had conducted an investigation to understand the potential exposure of customers' data. The Notice specifically stated that although M&T Bank claimed that "no information was obtained from M&T Bank's

internal systems" it stated that M&T Bank's investigation determined that certain information from undisclosed "external service providers" was compromised, including Plaintiff's information. Although M&T Bank claimed in the Notice that it did "not believe that this [data breach] presents elevated risk to you" it provided no facts or information to support the statement in the Notice. Notably, in the very next paragraph M&T Bank's Notice stated that it "will continue to closely monitor your accounts for potentially fraudulent activity" and that customers "consider signing up for credit monitoring from Equifax, which we've arranged at no cost to you for one year."

11. Since the announcement of the Data Breach, Plaintiff has spent considerable time mitigating her risk of identity theft and researching how to protect herself from such risk, including monitoring her accounts and credit, and implementing a credit freeze. Plaintiff has spent additional time researching the Data Breach and the potential risks therefrom and must continue to spend time monitoring her information and accounts.

12. Since receiving the Notice, Plaintiff has also received a significant increase in spam calls, as compared to prior to the Data Breach. Plaintiff has also suffered emotional distress as a result of her PII being accessed and exposed to unauthorized persons.

13. As a result of the Data Breach, Plaintiff will continue to be at a heightened and certainly impending risk for fraud and identity theft and will continue to suffer accompanying damages for years to come.

14. Defendant Progress is a Delaware corporation with its principal place of business located at 15 Wayside Rd., Suite 400, Burlington, Massachusetts 01803.

15. Defendant M&T Bank is a New York corporation with its principal place of business located at 1 M&T Plaza, Buffalo, New York 14203.

III. JURISDICTION & VENUE

16. This Court has jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

17. Absent the Court's MDL Order No. 12 (Direct Filing Order), Plaintiff Reardon could have filed her action directly in this District, as her claims arise, in part, from the actions and inactions of Progress described below. This action could also have been filed in the Western District of New York as Plaintiff's claims also arise, in part, from the actions and inactions of M&T Bank described below. The Western District of New York has personal jurisdiction over Defendant M&T Bank because it maintains its principal place of business in the District, and is authorized to conduct business in this District making it subject to general personal jurisdiction in New York. Additionally, the Western District of New York has personal jurisdiction over Defendant Progress because Progress has committed acts within the District that give rise to this action, and has established minimum contacts with this forum such that the exercise of jurisdiction over Progress aligns with traditional notions of fair play and substantial justice. The Western District of New York is the proper venue for this case pursuant to 18 U.S.C. § 1391(b)(1) because Defendant M&T Bank's principal place of business is located in the District; and pursuant to 18 U.S.C. § 1391(b)(2) because a substantial part of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

IV. FACTUAL BACKGROUND

A. Progress and the Services It Provides

18. Progress is a Massachusetts-based company that develops and sells a variety of software for businesses, including the secure file transfer application MOVEit. Progress advertises that more than 100,000 enterprises run business systems through its platforms, and 6 million business users work with apps running on Progress's technologies.[3]

19. Progress's various business and government customers retain sensitive information including, but not limited to, bank account information, addresses, driver's license numbers, dates of birth, and social security numbers, and use Progress's MOVEit product to securely transfer files containing that sensitive information.

20. While administering these services, Progress receives, handles, and collects consumer PII, including without limitation, full names, addresses, and bank account numbers.

21. By obtaining, collecting, and storing Plaintiff's and the Class Members' PII, Progress knew, or should have known, that it was a prime target for hackers given the significant amount of sensitive personally identifiable information processed through its customers' computer data and storage systems. Progress's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

22. Despite knowing the prevalence of data breaches, Progress failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. Progress has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized

[3] *Company Overview*, PROGRESS, https://investors.progress.com/?ga=2.130524045.306488999.1689141297-1144817577.1689141297&gl=Pklrbgt*ga*MTE0NDgxNzU3Ny4xNjg5MTQxMjk3*ga9JSNBCSF54*MTY4OTE0MzY0MC4yLjAuMTY4OTE0MzY0NC41Ni4wLjA (last visited June 4, 2024).

breaches. Progress failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

B. M&T Bank and the Services it Provides

23. M&T Bank is a New York company that offers a wide range of financial services to consumers, businesses, professional clients, governmental entities and financial institutions throughout New York, Maryland, New Jersey, Pennsylvania, Delaware, Connecticut, Massachusetts, Maine, Vermont, New Hampshire, Virginia, West Virginia, and the District of Columbia, as well as Ontario, Canada. As of December 31, 2023, M&T Bank reported $207.8 billion in total assets.

24. As part of its business operations, M&T Bank receives, handles, and collects consumer PII, including without limitation, full names, addresses, and M&T Bank checking, savings, and/or money market account numbers.

25. M&T Bank represents on its website under the heading "Cybersecurity Protection"[4] that it has "protective security measures" to protect customers from cybercriminals. Additionally, M&T Bank represents that it:

- maintains a comprehensive Enterprise Information Security Program that is shared with our Regulators and aligned with an industry standard incorporating five core functions:
    - Identify: Identify risks to systems, data and assets to prioritize the Bank's information security activities
    - Protect: Develop and implement safeguards to protect our customers' information
    - Detect: Implement technology to identify anomalies and events

[4] *See* M&T Bank Help Center, Bank Security Tips and Best Practices, https://www3.mtb.com/homepage/explore-the-m-and-t-bank-help-center/bank-security-tips-and-best-practices/how-mandt-protects-you/cybersecurity-protection.

- Respond: Create and utilize activities to limit the impact of a detected cybersecurity event
- Recover: Execute plans to restore and recover from a natural or man-made event

- M&T Bank employs multiple layers of security and defense including:
  - Network and location perimeter protection
  - Real time continuous monitoring and detection of security incidents
  - Vulnerability and penetration testing
  - Intrusion detection and prevention systems
- Policies and Standards:
  - M&T Bank develops and follows information security policies and standards to protect our customer and corporate information
- Information Security Awareness Program:
  - M&T Bank has a robust information security awareness program to help safeguard our customers' information and data
  - We continually train and educate our employees to ensure they understand cybersecurity risks, threats and the latest scams.

26. Moreover, M&T Bank represents on its website under the heading "Fraud Detection"[5] that it is proactively keeping customers' accounts safe with data monitoring technologies that recognize and alert customers to suspicious activities. Additionally, M&T Bank's website further states:

> M&T Bank employs enhanced technologies to provide the best protection for our customers. We continuously monitor accounts and cardholder activity and use data mining for fraud detection and prevention. Customers who opt into the free M&T Bank's Alerts service have the additional fraud monitoring advantage of being informed immediately if unusual account activity occurs. We'll send you an email or text if we detect suspicious activity, your PIN number changes, an online or phone transaction occurs or if a

[5] *See* M&T Bank Help Center, Bank Security Tips and Best Practices, Fraud Detection, https://www3.mtb.com/homepage/explore-the-m-and-t-bank-help-center/bank-security-tips-and-best-practices/fraud-detection.

> transaction is declined. We can then work together to identify potential fraud. The faster the reaction, the better our chances of stopping further damage and of recovering any losses.

27. Moreover, M&T Bank's Form 10-K filed with the Securities and Exchange Commission specifically addresses M&T Bank's data security policies and its oversight of its vendors such as Progress. Specifically, M&T Bank's Form 10-K filed on February 21, 2024[6] under the Section Item 1C. Cybersecurity represented:

- The Company has established policies, processes, controls and systems designed to identify, assess, measure, manage, monitor and report risks related to cybersecurity and help prevent or limit the effect of possible cybersecurity threats and attacks.
- The Company has also established processes to oversee and identify cybersecurity risks from third-party service providers.
- Third-party service providers (including suppliers and business partners) are required to have security policies, standards and procedures that meet or exceed the information security guidelines as specified in the Security Program.
- The Company has an established third-party due diligence program to ensure vendors meet the Company's expectations as agreed to in their contract. Roles, responsibilities and expectations for service providers and other third parties are communicated and documented through contracts (and other associated agreements) and monitored through oversight as part of the Company's Third-Party Risk Management Program.

28. By obtaining, collecting, and storing Plaintiff's and the Class Members' PII, M&T Bank knew, or should have known, that such data was a prime target for hackers given the

[6]*See* M&T Bank's Form 10-K (Feb. 21, 2024), https://www.board-cybersecurity.com/annual-reports/tracker/20240221-mt-bank-corp-cybersecurity-10k/.

significant amount of sensitive personally identifiable information processed through its customers' computer data and storage systems. Moreover, M&T Bank knew, or should have known, that the provision of Plaintiff's and Class Members' PII to vendors such as Progress required M&T Bank to exercise proper diligence and control over such vendors. Indeed, M&T Bank acknowledged in its Form 10-K filing the cybersecurity risks third party service providers like Progress presented. M&T Bank knew, or should have known, of these risks, and created a third party due diligence program to "ensure" vendors such as Progress met their expectations for cybersecurity. M&T Bank also knew, or should have known, of these risks because it admitted that it monitored and oversaw vendors such as Progress through its Third-Party Risk Management Program. Furthermore, M&T Bank's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

29. Despite knowing the prevalence of data breaches, M&T Bank failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its customer's PII, whether through its own systems or those of its vendors. M&T Bank has the resources to prevent a breach, but neglected to adequately invest in data security and vendor vetting, despite the growing number of well-publicized breaches. M&T Bank failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

C. The Data Breach

30. A notice dated August 2023 was sent to Plaintiff Reardon by M&T Bank which stated ("Notice"):

> We're writing to let you know about a recent global cybersecurity incident involving MOVEit, a file transfer tool owned by Progress Software…Once we learned of this incident, we immediately began

> an investigation to understand the potential exposure of our customers' data…Our investigation did [] determine that certain information at our external service providers was compromised, including some of your information.

31. According to the Notice, the breach resulted in individuals' names, addresses, and checking, savings, and/or money market account number(s) being compromised and acquired by unauthorized actors.

32. Plaintiff is informed and believes that certain categories of PII she provided were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed and believes that criminals would have no purpose for hacking Defendants' software other than to exfiltrate, steal, destroy, use, or modify as part of their ransom attempts, the coveted personally identifiable information stored or processed by Defendants' customers.

33. The personally identifiable information exposed by Defendants as a result of their inadequate data security and/or inadequate oversight of vendors' data security policies and lax third party risk management program left Plaintiff's and the Class' PII at risk of being bought and sold on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personally identifiable information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

34. When malicious actors infiltrate companies and exfiltrate the personally identifiable information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

35. The harm resulting from a data breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes as compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

36. The information compromised in this unauthorized cybersecurity attack involves sensitive PII, which is significantly more valuable to consumers than the loss of, for example, credit card information in a retailer data breach because, there, consumer victims can cancel or close credit and debit card accounts; whereas here, the information compromised such as full names, addresses, and M&T Bank checking, savings, and/or money market account numbers (are difficult, if not impossible, to change.

37. Indeed, once PII is stolen, it is then sold to cybercriminals who use it to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personally identifiable information being harvested from the victim, as well as the personally identifiable information of the original victim's family, friends, and colleagues.

38. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personally identifiable information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personally identifiable information to others who do the same.

39. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personally identifiable information have been sold at prices ranging from $40 to $200, and bank details at a price range of $50 to $200.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[8] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[9]

40. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[10] Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

41. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

---

[7] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.Digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[8] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web,* EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[9] *In the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 4, 2024).

[10] *See* Jon Fingas, *Fraud ring uses stolen data to scam unemployment insurance programs*, ENGADGET (May 17, 2020), https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* Lily Hay Newman, *The Nigerian Fraudsters Ripping off the Unemployment System*, WIRED (May 19, 2020), https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

42. Identity thieves can use PII, such as that of Plaintiff and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

43. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

[11] U.S. Gen. Accounting Office, *GAO-07-737, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 29 (2007), http://www.gao.gov/new.items/d07737.pdf (last visited June 4, 2024).

45. When cyber criminals access financial information and other PII – as they did here – there is no limit to the amount of fraud to which Defendants may have exposed Plaintiff and Class Members.

46. Federal and state governments have established security standards and have issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the FTC has issued guidance for businesses that highlight the importance of reasonable data security practices.

47. According to the FTC, the need for data security should be factored into all business decision-making.[12] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[13] Among other things, the guidelines note that businesses should properly dispose of personally identifiable information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

48. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for

[12] *See* Federal Trade Commission, *Start with Security: A Guide For Business* (2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited June 4, 2024).

[13] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited June 4. 2024).

suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[14]

49. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personally identifiable information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45.

50. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Defendants' failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed at protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as Defendants that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personally identifiable information that they collect and maintain. Accordingly, Defendants knew or should have known that its customers' information was a prime target for hackers.

52. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2021, there were 4,145 publicly disclosed data

[14] *See id*.

breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[15]

53. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud as compared to 5.7 million people in 2021.[16]

54. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[17]

55. Upon information and belief, Defendants did not encrypt Plaintiff's and Class Members' personally identifiable information involved in the Data Breach.

56. As detailed above, Defendants are large, sophisticated software and banking companies with the resources to deploy robust cybersecurity protocols. Defendants knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiff and Class Members. Their failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*: (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that their customer's or vendor's network

[15] *2021 Year End Report—Data Breach*, FLASHPOINT (Feb. 4, 2022), https://flashpoint.io/resources/research/2021-year-end-report-data-breach-quickview/.

[16] *Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 4, 2024).

[17] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, SECURITY (Oct. 29, 2021), https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-data-breach.

servers were protected against unauthorized intrusions when using the MOVEit program; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to provide customers, and therefore Plaintiff and Class members, with prompt and accurate notice of the Data Breach.

Plaintiff Reardon's Experience

57. Plaintiff Reardon began banking with M&T Bank in approximately 2022 after it took over her previous bank, People's United Bank. As a condition of banking with M&T Bank, Plaintiff Reardon's PII was provided to M&T Bank.

58. Plaintiff Reardon had no say in the vendor that M&T Bank used to process and transfer valuable and sensitive customer information, including PII.

59. As a result of the vulnerability in Progress's MOVEit product, the information Plaintiff Reardon provided to M&T Bank was among the data accessed and exfiltrated by an unauthorized third party in the Data Breach.

60. At all relevant times, Plaintiff Reardon is and was a member of the Class as defined herein.

61. Plaintiff Reardon's PII was exposed in the Data Breach because Defendants failed to safeguard her PII at the time of the Data Breach.

62. In August 2023, Plaintiff Reardon received the Notice from M&T Bank, stating that her name, address, and M&T Bank checking, savings, and/or money market account numbers were accessed in the Data Breach.

63. Since the Data Breach, Plaintiff Reardon has caught at least five different attempts to make fraudulent charges using her information. Plaintiff Reardon received a text message from

her bank asking her to verify each of these purchases, which alerted her to the fraudulent activity on her accounts.

64. Plaintiff Reardon has also experienced a significant uptick in the amount of spam emails, texts, and robocalls she receives since the Data Breach occurred.

65. As a result, Plaintiff Reardon has spent 72 hours to date dealing with the consequences of the Data Breach, which included and continues to include, researching the Data Breach; freezing her credit at the major credit bureaus; signing up for credit monitoring and identity theft insurance; changing passwords and resecuring her own computer network; contacting financial institutions, including to set up two-factor authentication for her bank accounts; self-monitoring her accounts for any indication of fraudulent activity, which may take years to detect; and, seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

66. Plaintiff Reardon's PII has value which can be determined based upon multiple sources. Although her data was shared with a third party, she did not receive any payment or compensation for the disclosure of her information. She suffered actual injury in the form of loss of value of her PII—a form of intangible property that she entrusted to M&T Bank, which was compromised in and as a result of the Data Breach.

67. Plaintiff Reardon suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her PII.

68. Plaintiff Reardon has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII, in combination with her name, now in the hands of unauthorized third parties/criminals.

69. Plaintiff Reardon has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

70. As a direct and foreseeable result of Defendants' negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of their systems, Plaintiff and Class Members, have suffered harm in that their sensitive PII has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the Data Breach.

71. Plaintiff and Class Members are well aware that their sensitive PII, which includes their banking information, is at risk of being available to other cybercriminals on the dark web. Accordingly, Plaintiff and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the Data Breach. Additionally, Plaintiff and Class Members have incurred, and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

V. CLASS ACTION ALLEGATIONS

72. Plaintiff brings this action on behalf of herself and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiff seeks to represent the following Class:

> All persons in the United States and its territories whose personally identifiable information was compromised in or as a result of Defendants' Data Breach which was discovered on or about May or June 2023 (the "Class").

73. Excluded from the Class are: Defendants and their parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

74. Plaintiff reserves the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

75. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below.

76. Numerosity: The potential members of the Class as defined are so numerous that the joinder of all members of the Class is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiff believes the cybersecurity breach affected millions of individuals nationwide.

77. Commonality: There are questions of law and fact common to Plaintiff and the Class that predominate over any questions affecting only the individual members of the Class. The common questions of law and fact include, but are not limited to, the following:

(a) whether Defendants had a duty to protect the PII of Plaintiff and Class Members;

(b) whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

(c) whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

(d) whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

(e) whether Defendants owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personally identifiable information being transferred through the MOVEit program;

(f) whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of personally identifying information of Class Members being transferred through the MOVEit program;

(g) whether Defendants acted negligently in connection with the vulnerabilities in the MOVEit program that allowed unauthorized access to Plaintiff's and Class Members' personally identifiable information;

(h) whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' personally identifiable information secure and prevent loss or misuse of that personally identifiable information;

(i) whether Defendants adequately addressed and fixed the vulnerabilities in the MOVEit program which permitted the Data Breach to occur;

(j) whether Plaintiff and Class Members are entitled to credit monitoring and other monetary relief; and

(k) whether Defendants' failure to implement and maintain reasonable security procedures and practices constitutes a violation of the Federal Trade Commission Act, 15 U.S.C. §45(a).

78. Typicality: The claims of Plaintiff are typical of the claims of the Class Members because all had their personally identifiable information compromised as a result of Defendants' failure to implement and maintain reasonable security measures and the consequent Data Breach.

79. Adequacy of Representation: Plaintiff will fairly and adequately represent the interests of the Class. Counsel for Plaintiff is experienced and competent in class actions, as well as various other types of complex and class litigation.

80. Superiority and Manageability: A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder is not practicable, and questions of law and fact common to Plaintiff predominate over any questions affecting only Plaintiff. Plaintiff has been damaged and is entitled to recovery by reason of Defendants' unlawful failure to adequately safeguard her data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most class members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on their own behalf pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as Defendants' records will readily enable the Court and Parties to ascertain affected companies and their employees.

81. Predominance: Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and

injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

82. Injunctive Relief: Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

83. Ascertainability: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendants' books and records.

84. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

85. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

(a) whether Defendants owed a legal duty to Plaintiff and Class Members to maintain security in the transfer of their personally identifiable information;

(b) whether Defendants breached that legal duty to Plaintiff and Class Members to exercise due care in maintaining security in the transfer of their personally identifiable information;

(c) whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

(d) whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personally identifiable information compromised in the breach; and

(e) whether Class Members are entitled to actual damages, credit monitoring, injunctive relief, and/or statutory damages, as a result of Defendants' wrongful conduct as alleged herein.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

NEGLIGENCE
(On Behalf of Plaintiff and the Class Against all Defendants)

86. Plaintiff realleges and incorporates by reference the preceding paragraphs 1 through 85 as if fully set forth herein.

87. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII, including securing the data being transferred through the MOVEit product from being compromised, stolen, accessed, and/or misused by unauthorized persons.

88. Defendants have a common law duty to prevent foreseeable harm to others. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personally identifiable information that were compliant with and/or better than industry-standard practices.

89. Defendants' duties included a duty to design, maintain, and test their security systems or the security systems of their customers and vendors to ensure that Plaintiff's and Class

Members' personally identifiable information was adequately secured and protected, to implement processes that would detect a breach of their security systems in a timely manner, to timely act upon warnings and alerts, including those generated by their own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify their clients, Plaintiff, and Class Members of any data breach.

90. Defendants' duties to use reasonable care arose from several sources, including but not limited to those described below.

91. Defendants' duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personally identifiable information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants also knew that it was more likely than not that Plaintiff and other Class Members would be harmed.

92. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' personally identifiable information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' personally identifiable information from disclosure.

93. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their personally identifiable information.

94. Defendants breached the duties that they owed to Plaintiff and Class Members described above and thus was negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personally identifiable information of Plaintiff and Class

Members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry standards; (e) timely disclose that Plaintiff's and Class Members' personally identifiable information in Defendants' possession had been or was reasonably believed to have been stolen or compromised; and (f) failing to comply fully even with its own purported security practices.

95. Defendants knew or should have known of the risks of transferring personally identifiable information through its product and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of Defendants' operations further shows that Defendants knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. Upon information and belief, this is but one of the several vulnerabilities that plagued Defendants' systems and led to the Data Breach.

96. Through Defendants' acts and omissions described in this complaint, including Defendants' failure to provide adequate security and their failure to protect the personally identifiable information of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' personally identifiable information.

97. Defendants further failed to timely and accurately disclose to clients, Plaintiff, and Class Members that their personally identifiable information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web. Plaintiff and Class Members could have taken action to protect their personally identifiable information if they were provided timely notice.

98. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their personally identifiable information would not have been compromised.

99. Plaintiff and Class Members relied on Defendants to keep their personally identifiable information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

100. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory and nominal damages, in an amount to be proven at trial. As a result of Defendants' failure to protect PII, Plaintiff's and Class Members' PII has been accessed by malicious cybercriminals. Plaintiff's and the Class Members' injuries include:

(a) theft of their PII;

(b) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

(c) costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

(d) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personally identifiable information being placed in the hands of criminals;

(e) damages to and diminution of value of the PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's

and the Class Members' data against theft and not allow access and misuse of their data by others;

(f) continued risk of exposure to hackers and thieves of their personally identifiable information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the Data Breach;

(g) emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members;

(h) loss of the inherent value of their PII;

(i) the loss of the opportunity to determine for themselves how their personally identifiable information is used; and,

(j) other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

101. In connection with the conduct described above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class Members would suffer if their highly sensitive and confidential PII, including but not limited to name, address, and financial account numbers was accessed by unauthorized third parties.

SECOND CLAIM FOR RELIEF

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class Against all Defendants)

102. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 101 as if fully set forth herein.

103. Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personally identifiable information by companies such as Defendants. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based on the FTC Act that also create a duty.

104. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect personally identifiable information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personally identifiable information it obtained and stored and the foreseeable consequences of a data breach.

105. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

106. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

107. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

108. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by unauthorized persons;

h. continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

109. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant M&T Bank)

110. Plaintiff realleges and incorporates by reference the preceding paragraphs 1 through 109 as if fully set forth herein.

111. M&T Bank provides specific representations to its customers concerning its cybersecurity practices. These promises were made to customers on its website since at least 2021.[18]

112. The provisions of M&T Bank's "Cybersecurity Protection" Promises provide that "M&T Bank Corporation maintains a comprehensive Enterprise Information Security Program that is shared with our Regulators and aligned with an industry standard incorporating five core functions." *Id.* Those functions are:

- Identify: Identify risks to systems, data and assets to prioritize the Bank's information security activities
- Protect: Develop and implement safeguards to protect our customers' information
- Detect: Implement technology to identify anomalies and events
- Respond: Create and utilize activities to limit the impact of a detected cybersecurity event

[18] *See* Cybersecurity Protection, M&T Bank (2021), https:// web.archive.org/web/20221001085617/https://www3.mtb.com/homepage/explore-the-m-and-t-bank-help-center/bank-security-tips-and-best-practices/how-mandt-protects-you/cybersecurity-protection. This Court has previously cited to archive.org ("The Way Back Machine") as a resource to review prior versions of websites. *See, e.g., Tassinari v. Salvation Army Nat'l Corp.*, 610 F. Supp. 3d 343, 354 (D. Mass. 2022).

- Recover: Execute plans to restore and recover from a natural or man-made event

Id.

113. Additionally, M&T Bank states that it "employs multiple layers of security and defense" including:

- Network and location perimeter protection
- Real time continuous monitoring and detection of security incidents
- Vulnerability and penetration testing
- Intrusion detection and prevention systems

Id.

114. M&T Bank also states that it "develops and follows information security policies and standards to protect our customer and corporate information" and has a "Security Awareness Program," which provides:

- M&T has a robust information security awareness program to help safeguard our customers' information and data
- We continually train and educate our employees to ensure they understand cybersecurity risks, threats and the latest scams

Id.

115. These express representations were made to Plaintiff and Class members, who were parties to such contracts, as it was their Private Information that defendant M&T Bank agreed to receive, store, utilize, transfer, and protect through their services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

116. Defendant M&T Bank made explicit representations concerning the safety and security of their systems, while at the same time not ensuring the safety and security of the applications they used to transfer information.

117. Defendant M&T Bank knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

118. Defendant M&T Bank breached its contracts with customers by, among other things, failing to adequately secure Plaintiff and Class Members' Private Information, and, as a result, Plaintiff and Class Members were harmed by defendant M&T Bank's failure to secure their Private Information.

119. As a direct and proximate result of the Data Breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

120. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

121. Plaintiff and Class Members are also entitled to injunctive relief requiring defendants M&T Bank to, *e.g.,* (i) strengthen their data security systems and monitoring procedures, especially for external service providers; (ii) submit to future annual audits of those

systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH CLAIM FOR RELIEF

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant Progress)

122. Plaintiff realleges and incorporates by references preceding paragraphs 1 through 121 as if fully set forth herein.

123. Upon information and belief, Progress entered into contracts with its government and corporate customers to provide secure file transfer services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to it.

124. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Defendants agreed to receive, store, utilize, transfer, and protect through their services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class members were direct and express beneficiaries of such contracts.

125. Progress knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

126. Progress breached these contracts by, among other things, failing to adequately secure Plaintiff and Class members' PII, and, as a result, Plaintiff and Class members were harmed by Defendants' failure to secure their PII.

127. As a direct and proximate result of the Data Breach, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred

mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their PII, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

128. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

129. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

FIFTH CLAIM FOR RELIEF

BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class Against all Defendants)

130. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 129 as if fully set forth herein.

131. As described above, Plaintiff and Class members were third-party beneficiaries under the contracts with and/or between Defendants.

132. Inherent in every contract is that implied covenant of good faith and fair dealing, which Defendants violated when they failed to maintain reasonable data security protocols, leading

to the disclosure of Plaintiff's and Class members' PII for purposes not required or permitted under the contracts.

133. Plaintiff and Class members have been injured by Defendants' conduct, incurring the harms and injuries arising from the Data Breach now and in the future and are entitled to the losses and damages they have sustained as a direct and proximate result thereof, as well as their costs and attorneys' fees incurred in this action.

SIXTH CLAIM FOR RELIEF

INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Class Against all Defendants)

134. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 133 as if fully set forth herein.

135. Defendants intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class members by intentionally configuring their systems in such a way that left Defendants vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class members' personally identifiable information.

136. Defendants' conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class members' personally identifiable information.

137. At all times, Defendants were aware that Plaintiff's and Class members' personally identifiable information in their possession contained highly sensitive and confidential personally identifiable information.

138. Plaintiff and Class members have a reasonable expectation of privacy in their personally identifiable information, which also contains highly sensitive medical information.

139. Defendants intentionally configured their systems in such a way that stored Plaintiff's and Class members' personally identifiable information to be left vulnerable to malware/ransomware attack, without regard for Plaintiff's and Class members' privacy interests.

140. The disclosure of the sensitive and confidential personally identifiable information of thousands of consumers was highly offensive to Plaintiff and Class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

141. Defendants' conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. Defendants' conduct would be especially egregious to a reasonable person as Defendants publicly disclosed Plaintiff's and Class members' sensitive and confidential personally identifiable information without their consent, to an "unauthorized person," i.e., hackers.

142. As a result of Defendants' actions, Plaintiff and Class members have suffered harm and injury, including but not limited to, an invasion of their privacy rights.

143. Plaintiff and Class members have been damaged as a direct and proximate result of Defendants' intrusion upon seclusion and are entitled to just compensation.

144. Plaintiff and Class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

SEVENTH CLAIM FOR RELIEF

INVASION OF PRIVACY (PUBLIC DISCLOSURE OF PRIVATE FACTS)
(On Behalf of Plaintiff and the Class Against all Defendants)

145. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 144 as if fully set forth herein.

146. Plaintiff and Class members had a reasonable expectation of privacy in the PII Defendants mishandled.

147. As a result of Defendants' conduct, publicity was given to Plaintiff's and Class members' PII, which necessarily includes matters concerning their private life.

148. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class members' PII to be highly offensive.

149. Plaintiff's and Class members' PII is not of legitimate public concern and should remain private.

150. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiff and Class members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

151. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

152. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

EIGHTH CLAIM FOR RELIEF

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against all Defendants)

153. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 152 as if fully set forth herein.

154. Plaintiff and Class members have both a legal and equitable interest in their PII that was collected by, stored by, and maintained by Defendants—thus conferring a benefit upon Defendants—that was ultimately compromised by the Data Breach.

155. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII.

156. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class members' PII; these cost savings increased the profitability of the services.

157. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

158. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class members

because Defendants failed to implement appropriate data management and security measures that are mandated by federal, state, and local laws, as well as industry standards.

159. Defendants should be compelled to provide, for the benefit of Plaintiff and Class members, all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

NINTH CLAIM FOR RELIEF

VIOLATION OF MASSACHUSETTS GENERAL LAWS, CHAPTER 93A (On Behalf of Plaintiff and the Class Against Defendant Progress)

160. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 159 as if fully set forth herein.

161. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

162. Plaintiff alleges that defendant Progress committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

163. Defendant Progress knew or should have known of the inherent risks in experiencing a data breach if Progress failed to maintain adequate systems and processes for keeping Plaintiff's and Class members' PII safe and secure. Only defendant Progress was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and the Class resulting from a data security incident such as the Data Breach; instead, Progress failed to implement such safeguards.

164. Defendant Progress's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant Progress's misconduct

included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

165. Defendant Progress acknowledges its conduct created actual harm to Plaintiff and Class members because Progress instructed them to monitor their accounts for fraudulent conduct and identity theft.

166. Defendant Progress knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PII and the importance of adequate security because of, inter alia, the prevalence of data breaches.

167. Defendant Progress failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff's and Class members' PII, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiff and Class members in a timely manner that their Private Information was accessed in the Data Breach.

168. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

169. As a direct and proximate result of Defendant Progress's unfair acts and practices, Plaintiff and the Class have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or fraudulent use of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendant's Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or

tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession (and/or to which Defendant continues to have access) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PII.

170. Neither Plaintiff nor the other Class members contributed to Defendant's Data Breach.

171. Plaintiff sent a demand for relief, in writing, to Defendant prior to filing this complaint. Multiple plaintiffs in consolidated actions have sent[19]—or alleged in their complaints that they would send[20]—similar demand letters as required by M.G.L. ch. 93A § 9. Plaintiff has not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiff and the Class.

---

[19] *See, e.g.*, *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[20] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp.*, 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al.*, 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al.*, 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al.*, 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al.*, 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al.*, 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al.*, 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al.*, 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al.*, 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al.*, 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al.*, 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al.*, 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al.*, 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al.* 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al.*, 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp.*, 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al.*, 23-cv-1913 (D. Md.).

172. Based on the foregoing, Plaintiff and the Class members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

173. Pursuant to M.G.L. ch. 231, § 6B, Plaintiff and Class members are further entitled to pre-judgment interest as a direct and proximate result of defendant Progress's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Plaintiff and Class members are entitled to interest in an amount according to proof.

TENTH CLAIM FOR RELIEF

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class Against all Defendants)

174. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 173 as if fully set forth herein.

175. Under the Declaratory Judgment Act, 28 U.S.C. §§2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as the ones alleged here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

176. An actual controversy has arisen in the wake of the Defendants' Data Breach regarding its present and prospective common law and other duties to reasonably safeguard consumers' personal identifying information being transferred through its secure file transfer program, and regarding whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their personally identifiable information. Plaintiff and Class Members continue to suffer an injury as a

result of the compromise of their personally identifiable information and remain at imminent risk that further compromises of their personally identifiable information will occur in the future.

177. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendants continue to owe a legal duty to secure consumers' personally identifiable information, including Plaintiff's and Class Members' personally identifiable information, and to timely notify them of a data breach under the common law, Section 5 of the FTC Act; and

(b) Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' personally identifiable information.

178. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' personally identifiable information.

179. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

180. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing

reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

181. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and the thousands of Class Members whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, pray for the following relief:

A. An order certifying the Class as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiff is a proper class representative and appointing Plaintiff's counsel as class counsel;

B. An order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. Permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial, in excess of $5,000,000;

E. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and,

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the putative Class, hereby demands a trial by jury on all issues of fact or law so triable.

DATED: July 23, 2024

Respectfully submitted,

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Floor
Boston, MA 02109
Tel: (617) 482-3700
kristenj@hbsslaw.com

Plaintiff's Liaison & Coordinating Counsel

Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Plaintiff's Lead Counsel

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo (Bar No. 671410)
Amanda M. Rolon
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
arolon@scott-scott.com

Counsel for Plaintiff